PCT / IB 0 3 / 0 2 9 4 5
25. 07. 03
Rec'd PCT/PTO 19 JAN 2005

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 54 747.5

Anmeldetag: 23. November 2002

Anmelder/Inhaber: Philips Intellectual Property & Standards GmbH, Hamburg/DE

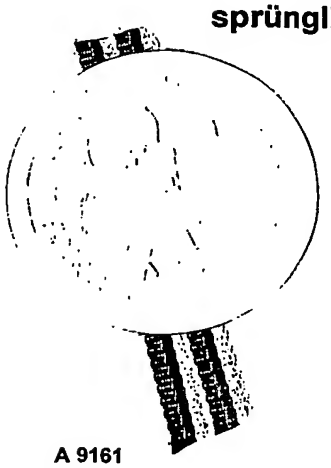
vormals: Philips Corporate Intellectual Property GmbH

Bezeichnung: Sicherheitssystem für Geräte eines drahtlosen Netzwerks

Priorität: 29. Juli 2002 DE 102 34 643.7

IPC: H 04 L 9/08

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 2. Juli 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Jerofsky

A 9161
03/00
EDV-L

ZUSAMMENFASSUNG

Sicherheitssystem für Geräte eines drahtlosen Netzwerks

Die Erfindung bezieht sich auf ein Sicherheitssystem für drahtlose Netzwerke mit einer tragbaren Einheit (1) mit einer Schlüsseleinheit (3) zur Bereitstellung eines Schlüsseldatensatzes (4, 17, 104), die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4, 17, 104) vorgesehen ist. In wenigstens einem drahtlosen Gerät (2) des Netzwerks ist eine Empfangseinheit (7) vorgesehen, die einen Empfänger (9) zum Empfang des Schlüsseldatensatzes (4) und eine Auswertekomponente (11) des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes (4, 17, 104) oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist. Durch den Schlüsseldatensatz erlangen die Geräte des drahtlosen Netzwerks einen gemeinsamen geheimen Schlüssel, mit Hilfe dessen die Ver- und Entschlüsselung der übertragenen Nutzdaten und/oder die Authentifizierung vorgenommen wird. Die Einheit (101) kann ferner eine Leseeinrichtung (107) für eine Chipkarte (108) enthalten, wobei die Chipkarte (108) vorzugsweise den Dekodier-Schlüsseldatensatz (104) eines Kopierschutzes digitaler Daten enthält.

Fig. 1

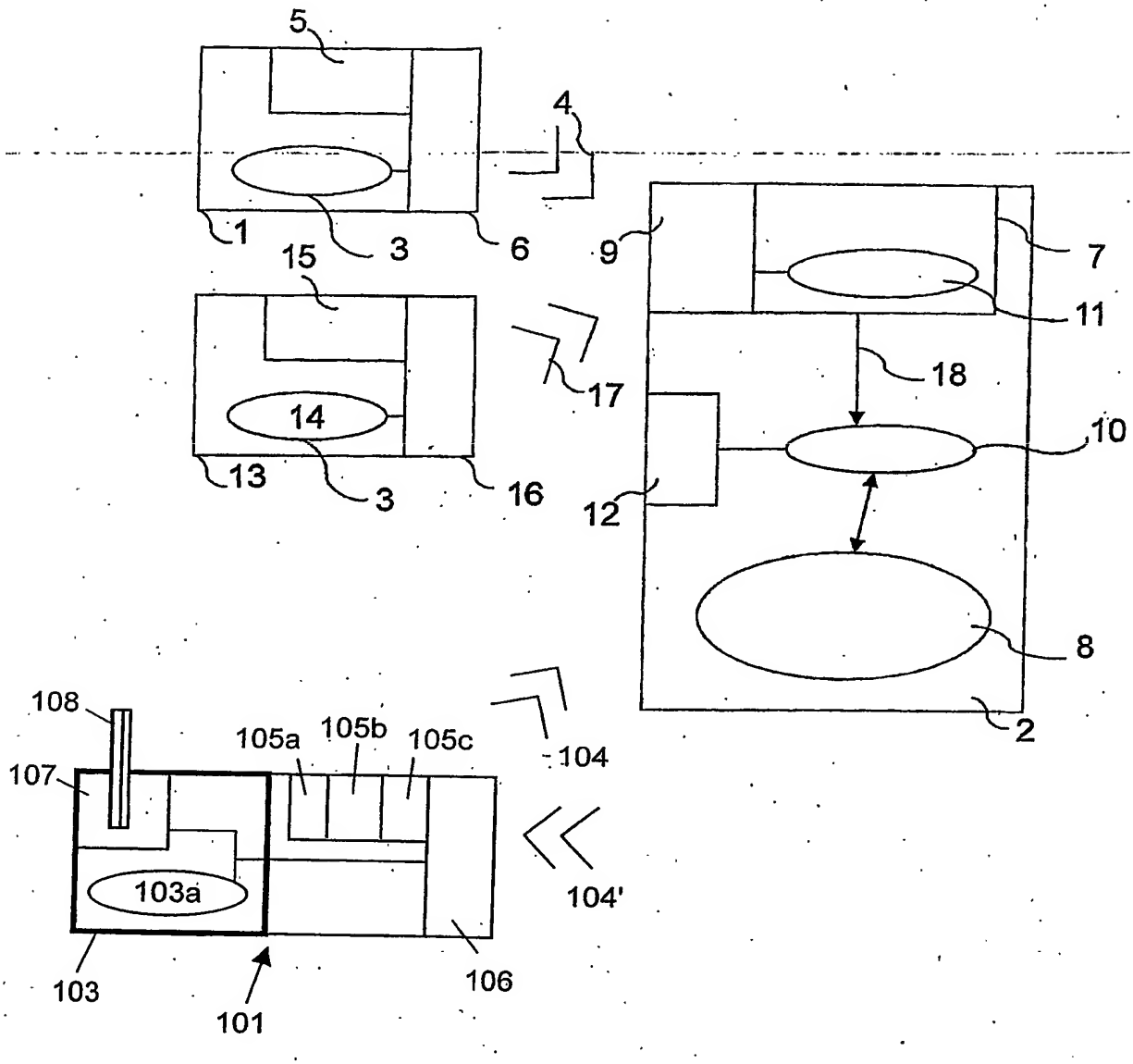

5
4
1
3
6
9
7
11
15
18
17
14
10
13
3
16
12
8
2
108
105a
105b
105c
104
107
104'
103a
103
101
106

FIG. 1

BESCHREIBUNG

Sicherheitssystem für Geräte eines drahtlosen Netzwerks

Die vorliegende Erfindung bezieht sich allgemein auf ein Sicherheitssystem für Netzwerke, insbesondere drahtlose Netzwerke.

Der Einsatz von drahtloser Kommunikation zur Unterstützung mobiler Geräte (wie Schnurlostelefone) oder als Ersatz für drahtgebundene Lösungen zwischen stationären Geräten (z. B. PC und Telefonanschlussdose) ist schon heute weit verbreitet.

Für zukünftige digitale Hausnetzwerke bedeutet das, dass sie typischerweise nicht nur aus mehreren drahtgebundenen Geräten, sondern auch aus mehreren drahtlosen Geräten bestehen. Bei der Realisierung digitaler drahtloser Netzwerke, insbesondere Hausnetzwerke, werden Funktechnologien wie Bluetooth, DECT und vor allem der IEEE802.11 Standard für "Wireless Local Area Network" verwendet. Drahtlose Kommunikation kann auch über Infrarot (IrDA) erfolgen.

Desgleichen werden auch andere der Information oder Unterhaltung der Nutzer dienende Netze zukünftig unter anderem auch drahtlos kommunizierende Geräte enthalten. Insbesondere seien hier sogenannte Ad-hoc-Netzwerke genannt, bei denen es sich um temporär eingerichtete Netzwerke mit im Allgemeinen Geräten verschiedener Besitzer handelt. Ein Beispiel solcher Ad-hoc-Netzwerke findet sich in Hotels: ein Gast wird z. B. die Musikstücke auf seinem mitgebrachten MP3-Spieler über die Stereoanlage des Hotelzimmers wiedergeben wollen. Ein weiteres Beispiel sind alle Arten von Treffen, bei denen sich Menschen mit drahtlos kommunizierenden Geräten zum Austausch von Daten oder Medieninhalten (Bilder, Filme, Musik) zusammen finden.

Bei Verwendung von Funktechnologien können Geräte wie z.B. ein MP3-Speicher-Gerät und eine HiFi-Anlage drahtlos über Funkwellen als Datenleitung miteinander kommunizieren. Prinzipiell gibt es dabei zwei Betriebsarten. Entweder kommunizieren die Geräte direkt von Gerät zu Gerät (als Peer-to-Peer-Netzwerk) oder über einen zentralen Zugangspunkt (Access Point) als Verteilerstation.

Je nach Standard haben die Funktechnologien Reichweiten von mehreren 10 Metern in Gebäuden (IEEE802.11 bis zu 30m) und mehreren 100 Metern im Freien (IEEE802.11 bis zu 300m). Funkwellen durchdringen auch die Wände einer Wohnung oder eines Hauses. Im Abdeckungsbereich eines Funknetzes, also innerhalb der Reichweite können die übertragenen Informationen prinzipiell von jedem Empfänger, der mit einer entsprechenden Funkschnittstelle ausgerüstet ist, empfangen werden.

Daraus ergibt sich die Notwendigkeit, drahtlose Netzwerke gegen unbefugtes oder auch unbeabsichtigtes Abhören der übertragenen Informationen, sowie gegen unbefugten Zugang zum Netzwerk und damit zu dessen Ressourcen besonders zu schützen.

Methoden zur Zugangskontrolle und zum Schutz der übertragenen Informationen sind in den Funkstandards enthalten (z.B. bei IEEE802.11 in " IEEE802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Standard, IEEE", New York, August 1999, Kapitel 8). Allgemein in Funknetzen als auch speziell im IEEE802.11 Standard beruht jede Form der Datensicherheit letztlich auf geheimen Verschlüsselungscodes (Schlüsseln) oder Kennworten, die nur den befugten Kommunikationspartnern bekannt sind.

Zugangskontrolle bedeutet, zwischen befugten und unbefugten Geräten unterscheiden zu können, d.h. ein Zugang gewährendes Gerät (z.B. ein Access Point, oder ein Gerät eines Heim- oder Ad-hoc-Netzwerks, das eine Kommunikationsanforderung erhält) kann anhand von übermittelten Informationen entscheiden, ob ein Zugang forderndes Gerät befugt ist. Bei einem Medium wie Funk, das leicht abgehört werden kann, ist dabei die

einfache Übertragung von Zugangscodes oder die Verwendung von Identifikatoren (die vom Zugang gewährenden Gerät mit einer Liste von Identifikatoren befugter Geräte verglichen werden kann) unzureichend, da ein unbefugtes Gerät durch Mithören dieser Übertragung unberechtigt an die notwendigen Zugangsinformationen gelangen kann.

Das in Zusammenhang mit IEEE802.11 verwendete sogenannte MAC-Address-Filtering stellt in seiner einfachen Form keinen sicheren Schutz dar. Bei dieser Methode speichert der Access Point die Liste der MAC (Media Access Control)-Adressen der zum Zugriff auf das Netzwerk befugten Geräte. Versucht ein unbefugtes Gerät auf das Netzwerk zuzugreifen, wird es aufgrund der dem Access Point unbekannten MAC-Adresse zurückgewiesen. Neben der für Hausnetzwerke inakzeptablen Benutzerunfreundlichkeit der notwendigen Wartung einer MAC-Adressen-Liste hat diese Methode vor allem den Nachteil, dass es möglich ist, MAC-Adressen vorzutäuschen. Somit muss es einem unbefugten Benutzer nur gelingen, Kenntnis einer "befugten" MAC-Adresse zu erhalten, was wiederum beim Belauschen des Funkverkehrs einfach möglich ist. Deshalb wird Zugangskontrolle mit einer Authentifizierung gekoppelt, die auf einem geheimen Schlüssel oder Kennwort beruht.

Im IEEE802.11 Standard ist die "Shared-Key-Authentifizierung" definiert, bei der sich ein befugtes Gerät durch die Kenntnis eines geheimen Schlüssels auszeichnet. Die Authentifizierung wird dann wie folgt vorgenommen: Um die Befugnis festzustellen, sendet das Zugang gewährende Gerät einen Zufallswert (Challenge), den das Zugang fordernde Gerät mit dem geheimen Schlüssel verschlüsselt und zurücksendet. Dadurch kann das Zugang gewährende Gerät die Kenntnis des Schlüssels und damit die Zugangsberechtigung verifizieren (diese Methode wird in seiner allgemeinen Form auch "Challenge-Response-Methode" genannt).

Bei der Verschlüsselung werden die übertragenen Informationen vom sendenden Gerät verschlüsselt und vom empfangenden Gerät entschlüsselt, so dass die Daten für einen unbefugt oder unbeabsichtigt Mithörenden wertlos sind. Der IEEE802.11 Standard

verwendet dazu die Verschlüsselungsmethode Wired Equivalent Privacy (WEP). Dabei wird ein allen Geräten des Netzwerks bekannter, aber sonst geheimer Schlüssel (40 Bit oder 104 Bit WEP-Schlüssel) verwendet, der als Parameter in den im IEEE802.11 Standard festgelegten Verschlüsselungsalgorithmus zur Verschlüsselung der zu übertragenden Daten eingeht.

Im Falle von WEP wird derselbe Schlüssel auch zur Authentifizierung verwendet. Neben "symmetrischen" Verschlüsselungsverfahren (mit einem "shared key") gibt es auch die sogenannten public/private key-Verfahren, bei denen jedes Gerät einen allgemein bekannten Schlüssel (public key) zum Verschlüsseln bereit stellt und einen dazugehörigen, nur diesem Gerät bekannten geheimen Schlüssel (private key) besitzt, der das Entschlüsseln der mit dem public key verschlüsselten Informationen ermöglicht.

Dadurch ist Abhörsicherheit ohne einen im Voraus bekannten gemeinsamen geheimen Schlüssel möglich. Bei Anwendung dieser Art von Verfahren ist es jedoch einem beliebigen Gerät möglich, unter Nutzung des allgemein bekannten Schlüssels die Kommunikation zu einem Gerät (z.B. einem Zugang gewährenden Gerät) aufzunehmen. Deshalb ist auch hier eine Authentifizierung zur Zugangskontrolle notwendig, die wiederum auf einem geheimen Schlüssel beruht, der im Voraus den Kommunikationspartnern bekannt sein muss.

Zur Erhöhung der Datensicherheit können Netzwerkgeräte Mechanismen zur Vereinbarung von temporären Schlüsseln beinhalten, also Schlüsseln, die nur eine festgelegte Zeitspanne lang zur Verschlüsselung verwendet werden, so dass nicht immer derselbe geheime Schlüssel verwendet wird. Der Austausch dieser temporären Schlüssel erfordert aber eine abhörsichere Übertragung, die wiederum zumindest einen ersten geheimen Schlüssel benötigt, der im Voraus den Kommunikationspartnern bekannt sein muss. Wesentlich für die Erfindung ist, dass auch die Datensicherheit durch Verschlüsselung auf einem (ersten) geheimen Schlüssel beruht, der im Voraus den Kommunikationspartnern bekannt sein muss.

Um ein Sicherheitssystem für drahtlose Netzwerke zu schaffen, ist deshalb ein Konfigurationsschritt notwendig, der allen relevanten Geräten einen geheimen Schlüssel (für Authentifizierung und/oder Verschlüsselung) zur Verfügung stellt.

Dabei ist eine Besonderheit drahtloser Netzwerke, dass dieser Schlüssel nicht als "Klartext" (unverschlüsselt) über die drahtlose Kommunikationsschnittstelle übertragen werden sollte, da sonst ein unbefugtes Gerät durch mithören unberechtigt an den Schlüssel gelangen kann. Zwar kann durch Kodierverfahren, wie Diffie-Hellman, die abhörsichere Vereinbarung eines gemeinsamen geheimen Schlüssels zwischen zwei Kommunikationspartnern über eine Funkschnittstelle erreicht werden. Um jedoch zu verhindern, dass ein unbefugten Gerät die Schlüsselvereinbarung mit einem (Zugang gewährenden) Gerät des Netzwerkes initiiert, muss auch dieses Verfahren mit einer Authentifizierung der Kommunikationspartner gekoppelt sein, was wiederum einen (ersten) geheimen Schlüssel erfordert, der im Voraus den Kommunikationspartnern bekannt sein muss.

Bei Schnurlostelefonen nach DECT-Standard ist ein erster Schlüssel bereits ab Werk in den Geräten (Basisstation und Hörer) gespeichert. Zur Anmeldung eines neuen Hörers an der Basisstation muss der Schlüssel (PIN-Nummer), der in der Basisstation gespeichert ist, vom Benutzer am neuen Hörer eingegeben werden. Da der Benutzer den Schlüssel dazu kennen muss, ist dieser z.B. auf Aufklebern an der Basisstation verfügbar.

IEEE 802.11 basierte Firmen- oder Campus-Netzwerke mit einer dedizierten Infrastruktur werden im allgemeinen von speziell ausgebildeten Systemadministratoren konfiguriert. Diese benutzen im allgemeinen System-Management-Rechner, die drahtgebundene Verbindungen zu jedem Access Point besitzen. Über diese drahtgebundenen (und damit quasi abhörsicheren) Verbindungen werden die geheimen Schlüssel (z.B. WEP-Schlüssel) zu den Access Points übertragen. Die Schlüsseleingabe an den Klienten (z.B. drahtlose Laptops) erfolgt von Hand.

Die Durchführung eines Konfigurationsschrittes zur Installation eines ersten geheimen Schlüssels wird zwar vorausgesetzt (und die notwendigen Konfigurationsschritte sind in Software-Schnittstellen definiert), aber die Realisierung ist nicht festgelegt. Der IEEE802.11 Standard beinhaltet dazu in Kapitel 8.1.2 folgendes Statement:"The required secret shared key is presumed to have been delivered to participating STAs (stations) via a secure channel that is independent of IEEE 802.11. The shared key is contained in a write only MIB (Management Information Base) attribute via the MAC management path."

Ein weiterer Problemkreis, der bei der drahtlosen Kommunikation zwischen Netzwerkkomponenten auftritt, betrifft die Sicherung bzw. den Schutz von Urheber- bzw. Eigentumsrechten an digitalen Informationen. Ein derartiger Schutz für digitale Daten wird durch ein sogenanntes Digital Rights Management (DRM) gewährleistet. So beruhen zum Beispiel Anwendungen wie "Pay TV" oder "Pay Per View" auf einem Dekodierschlüssel, welcher typischerweise auf einer Chipkarte hinterlegt ist, die auf dem herkömmlichen Postweg regelmäßig (z. B. monatlich) an Nutzer versandt wird. Zum Lesen der Chipkarte ist in einen Decoder ein Kartenlesegerät integriert, wobei der Decoder mit Hilfe des Dekodierschlüssels die Entschlüsselung von verschlüsselt übermittelten Daten des Informationsanbieters erlaubt. Die entschlüsselten Daten dürfen außerhalb des Dekodierers nicht unverschlüsselt gesendet werden, da sonst eine unberechtigte Verwendung der Daten unter Missachtung der Eigentumsrechte möglich wäre.

Auf der anderen Seite besteht jedoch bei Verbrauchern und Geräteherstellern der Wunsch, auch die Geräte eines drahtlosen Netzwerkes zur Wiedergabe von Informationen an beliebigen Orten nutzen zu können. Die hierzu erforderliche drahtlose Übermittlung der Informationen muss dabei jedoch vor einem Abhören und einem Missbrauch der Daten geschützt werden.

Der Erfindung liegt die Aufgabe zugrunde, eine benutzerfreundliche Installation eines geheimen Schlüssels in den Geräten eines vorzugsweise drahtlosen Netzwerks zu realisieren.

Die Aufgabe wird gelöst durch ein Sicherheitssystem für Netzwerke, insbesondere drahtlose Netzwerke, ausgestattet mit

- einer (ersten) tragbaren Einheit, die eine Schlüsseleinheit zur Bereitstellung eines Schlüsseldatensatzes enthält und die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist, und
- mindestens einer Empfangseinheit in wenigstens einem vorzugsweise drahtlosen Gerät des Netzwerks, die einen Empfänger zum Empfang des Schlüsseldatensatzes und eine Auswertekomponente des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.

Jedes drahtlose Gerät des Netzwerks hat sowohl eine Funkschnittstelle zum Übertragen von Nutzdaten als auch eine Empfangseinheit zum Empfang eines Schlüsseldatensatzes von einer ersten tragbaren Einheit. Zur Sicherung des drahtlosen Nutzdatenverkehrs zwischen den Geräten wird in jedes Gerät abhörsicher ein Schlüsseldatensatz eingegeben, durch den diese Geräte einen gemeinsamen geheimen Schlüssel erlangen, mit Hilfe dessen die Ver- und Entschlüsselung der übertragenen Nutzdaten und/oder die Authentifizierung vorgenommen wird. Mit dem gemeinsamen geheimen Schlüssel kann falls erforderlich auch ein drahtgebundener Austausch von Nutzdaten gesichert werden. Ferner kann der Schlüssel dazu dienen, Eigentumsrechte an digitalen Inhalten zu schützen, indem die zugehörigen Daten bis zum Endgerät mit einer speziellen Verschlüsselung des Eigentümers übermittelt werden können.

Der Schlüsseldatensatz wird von der Schlüsseleinheit der tragbaren Einheit , die über einen Sender oder einen Sender mit Detektoreinheit zur Kurzstreckenübertragung verfügt, bereitgestellt. Damit wird der Schlüsseldatensatz abhörsicher in jedes drahtlose Gerät des Netzwerkes eingegeben. Zur Auslösung einer Schlüsseldatensatzübertragung kann eine Taste an der Einheit dienen. Abhängig von dem verwendeten Verfahren zur Kurzstreckeninformationsübertragung kann die Auslösung einer Schlüsseldatensatzübertragung aber auch dadurch erfolgen, dass die Einheit in unmittelbare Nähe der Empfangseinheit gebracht wird und die Detektoreinheit die Schlüsseldatensatzübertragung auslöst.

Der Schlüsseldatensatz enthält als wesentlichen (und möglicherweise einzigen) Bestandteil einen geheimen Schlüsselcode ("Schlüssel"). Zum Empfang des Schlüsseldatensatzes verfügt jedes drahtlose Gerät des Netzwerkes über eine Empfangseinheit bestehend aus einem Empfänger und einer Auswertekomponente, die nach Erhalt des Schlüsseldatensatzes den Schlüssel extrahiert und diesen über eine interne Schnittstelle an die für die Ver- und Entschlüsselung der Nutzdaten zuständige zweite Komponente (z.B. die für die Steuerung der Funkschnittstelle zuständige Treibersoftware) weiterleitet.

Ein durch die tragbare Einheit verwendetes Verfahren zur Kurzstreckeninformationsübertragung kann auf modulierten magnetischen-, elektromagnetischen Feldern, sowie Infrarot- oder sichtbarem Licht, Ultra- oder Infraschall oder beliebigen anderen, in ihrer Reichweite kontrollierbaren Übertragungstechnologien basieren. Die Übertragung des Schlüsseldatensatzes kann auch durch ein mehrdimensionales Muster auf der Oberfläche des Senders realisiert werden, welches von der Empfangseinheit ausgelesen wird. Wesentlich für die Erfindung ist, dass eine Technologie mit sehr kurzer Reichweite (wenige Zentimeter) oder kurzer Reichweite und starker lokaler Begrenzung (z.B. Infrarot) benutzt wird, so dass die Eingabe der Schlüsseldatensatz aus einer sehr kurzen Distanz stattfindet und auf keinen Fall die Wände eines Raumes durchdringen kann.

Ein besonderer Vorteil dieser Lösung besteht darin, dass Unbefugten der Empfang des Schlüsseldatensatzes nicht möglich ist. Die Übertragung des Schlüsseldatensatzes kann durch einen Tastendruck an der tragbaren Einheit ausgelöst werden oder - z.B. bei Verwendung von Hochfrequenz-Transpondertechnologie (kontaktloser RF-tag Technologie) - auch dadurch, dass die tragbare Einheit in unmittelbarer Nähe der Empfangseinheit platziert wird. Somit ist das Eingeben des Schlüsseldatensatzes in ein Gerät für einen Benutzer durch Annähern der tragbaren Einheit an das Gerät (oder Richten der Einheit auf das Gerät) und eventuelles Betätigen einer Taste an der Einheit besonders einfach und unkompliziert. Der Benutzer benötigt auch keine Kenntnis über den Inhalt des Schlüsseldatensatzes bzw. den geheimen Schlüssel, Ein Fachmann für die Eingabe und die Administration des Schlüsseldatensatzes ist nicht notwendig. Die Benutzerfreundlichkeit ist ein weiterer besonderer Vorteil dieser Lösung.

Drahtlose Netzwerke, insbesondere Hausnetzwerke, sollten Zugriff nicht nur für ständige Benutzer des Hausnetzwerks (z.B: Eigentümer) bieten, sondern auch einen ggf. beschränkten Zugriff für temporäre Benutzer wie z.B. Gäste ermöglichen.

Eine vorteilhafte Weiterbildung der Erfindung besteht aus einer als Schlüsselgenerator bezeichneten Komponente, die in der Schlüsseleinheit enthalten ist und zur Erzeugung zusätzlicher Schlüsseldatensätze dient. Der Schlüsselgenerator ist eine zusätzliche Komponente der ersten tragbaren Einheit oder in einer zweiten separaten tragbaren Einheit realisiert.

Ein vom Schlüsselgenerator erzeugter Schlüsseldatensatz, sog. Gast-Schlüsseldatensatz, ist so aufgebaut, dass er immer (z.B. durch spezielle Bits im Schlüsseldatensatz) von einem z.B. im Speicher der Einheit gespeicherten (Heim-)Schlüsseldatensatz unterschieden werden kann. Ebenso ist bei einer Eingabe eines Schlüsseldatensatzes immer klar, ob ein Heim-Schlüsseldatensatz oder ein Gast-Schlüsseldatensatz eingegeben wird. Dazu hat die tragbare Einheit mit Speicher und Schlüsselgenerator mindestens zwei Tasten (eine, um die Übertragung des Heim-Schlüsseldatensatzes aus dem Speicher auszulösen und eine, um die Übertragung eines Gast-Schlüsseldatensatzes auszulösen). Ist der Schlüsselgenerator in einer separaten zweiten Einheit realisiert, so ist diese eindeutig (z.B. durch Farbe, Aufschrift etc.) von der Einheit mit dem Heim-Schlüsseldatensatz unterscheidbar.

Ein Gast-Schlüsseldatensatz wird benutzt, um Gästen Zugriff auf Ressourcen des Netzwerks zu gewähren. Dazu wird an allen betreffenden (das heißt für die Nutzung in Verbindung mit den Geräten des Gastes freigegebenen) Geräten des Hausnetzwerks und den Geräten des Gastes (die nicht zum Hausnetzwerk gehören) ein Gast-Schlüsseldatensatz eingegeben, mit Hilfe dessen die Geräte des Gastes (z.B. Laptop) mit den betreffenden Geräten des Hausnetzwerks kommunizieren können. In einer alternativen Ausprägung wird der Gastschlüsseldatensatz dem Netzwerk einmal bekannt gegeben (z.B. durch Eingeben in eines der zum Netzwerk gehörigen Geräte) und braucht dann bei Bedarf nur

noch in die Geräte des Gastes eingegeben zu werden; damit sind dann alle Geräte des Netzwerks für die Benutzung mit den Geräten des Gastes freigegeben. Die Steuerung, auf welche Daten innerhalb der freigegebenen Geräte der Gast Zugriff haben soll, muss an anderer Stelle erfolgen.

Um dem Benutzer die Kontrolle über die Dauer des gewährten Gast-Zugangs zum Hausnetz zu ermöglichen, wird automatisch nach einer festgelegten Zeitspanne oder durch Benutzer-Interaktion der Gast-Schlüsseldatensatz in den Geräten des Hausnetzwerks gelöscht. Eine Benutzer-Interaktion zur Löschung eines Gast-Schlüsseldatensatzes kann z.B. die nochmalige Eingabe des aktuellen Heim-Schlüsseldatensatzes, ein spezieller Tastendruck an den betroffenen Hausnetz-Geräten oder an einem der betroffenen Hausnetz-Geräte und nachfolgende automatische Information aller anderen betroffenen Hausnetz-Geräte durch dieses Gerät sein.

Um eine unbefugte Benutzung eines Gast-Schlüsseldatensatzes durch einen früheren Gast zu verhindern, erzeugt der Schlüsselgenerator nach einer festgelegten Zeitspanne (z.B. 60 Minuten) nach der letzten Gast-Schlüsseldatensatzübertragung automatisch einen neuen Gast-Schlüsseldatensatz nach dem Zufallsprinzip. Dadurch erhält ein neuer Gast einen anderen Gast-Schlüsseldatensatz als der vorherige, wodurch sichergestellt ist, dass der vorherige Gast die Anwesenheit des neuen Gastes nicht zum unbefugten Zugang zum Hausnetz ausnutzen kann.

Ad-hoc-Netzwerke stellen eine weitere Ausprägung drahtloser Netzwerke dar, in denen temporär eine Anzahl von Geräten zur Kommunikation in einem gemeinsamen Netzwerk freigegeben werden sollen. In ähnlicher Weise wie beim Gastzugriff auf Hausnetzwerke, bei dem mittels eines Gast-Schlüsseldatensatzes einzelne Gast-Geräte für den Zugriff auf das Hausnetzwerk freigegeben werden, sollen beim Ad-hoc-Netzwerk Geräte anderer Besitzer mit mindestens einem Gerät des Benutzers kommunizieren können. Dazu gibt der Benutzer einen Schlüsseldatensatz, hier Ad-hoc-Schlüsseldatensatz genannt, in alle Geräte des Ad-hoc-Netzwerks (seine eigenen und die der anderen Benutzer) ein. Der Ad-hoc-Schlüsseldatensatz kann in einer Ausprägung ein Gast-Schlüsseldatensatz sein, er kann aber auch als Ad-hoc-Schlüsseldatensatz eindeutig gekennzeichnet sein.

Es ist bevorzugt, dass die Schlüsseldatensätze aus Bitfolgen bestehen, wobei jede Bitfolge in einem vordefinierten Format (z.B. als 1024-Bit Sequenz) übertragen wird. Die gesamte Bitfolge oder ein Teil davon wird von der Empfangseinheit als Schlüssel weitergeleitet. Falls die Bitfolge neben dem Schlüssel zusätzliche Bits beinhaltet, so ist genau festgelegt, welcher Teil der Bitfolge als Schlüssel verwendet wird (z.B. die 128 low-order Bits) und welche Bits der Bitfolge welche zusätzlichen Informationen beinhalten. Weitere Informationen können dabei Kennzeichnungen sein, die über die Art des Schlüsseldatensatzes (Heim-, Gast-, Ad-hoc- oder Dekodier-) informieren oder Angaben über die Länge und Anzahl der Schlüsselcodes enthalten, falls mehrere Schlüsselcodes gleichzeitig übertragen werden. Im Falle dass die Empfangseinheit für weitere Anwendungen genutzt wird, kennzeichnen die zusätzlichen Bits auch die Verwendung der Bitfolge als Schlüsseldatensatz.

Damit in zwei benachbarten Hausnetzwerken nicht der gleiche (Heim-)Schlüssel verwendet wird, sollte dieser global eindeutig sein. Dies kann erreicht werden z.B. indem verschiedene Einheiten-Hersteller unterschiedliche Wertebereiche von Schlüsselcodes benutzen und innerhalb dieser Bereiche so weit wie möglich in keinen zwei Einheiten den gleichen Schlüsseldatensatz speichern.

Ein nach dem IEEE802.11 Standard arbeitendes Netzwerk ist ein weit verbreitetes Beispiel für drahtlose Hausnetzwerke. In einem IEEE802.11 Netzwerk kann der zu übertragene Schlüsseldatensatz einen oder mehrere Wired Equivalent Privacy (WEP) - Schlüssel enthalten.

Die Eingabe des (Heim-)Schlüsseldatensatzes kann auch in Schritten zur Konfiguration des Netzwerks stattfinden, so dass zu Beginn der Konfiguration die Eingabe/ Installation des Schlüsseldatensatzes verlangt wird. Dadurch ist während des gesamten Konfigurationsprozesses eine abhörsichere Kommunikation der Geräte untereinander, sowie eine Zugangskontrolle (befugt sind alle Geräte, die über den Schlüsseldatensatz verfügen) gewährleistet. Dies ist insbesondere vorteilhaft bei der Anwendung automatisierter Konfigurationsverfahren, d.h. Verfahren ohne Benutzer-Interaktion (basierend auf Mechanismen wie z.B. IPv6 Auto-Konfiguration und Universal Plug and Play (UPnP)).

In einer bevorzugten Ausführungsform ist die tragbare Einheit in eine Fernbedienung eines Gerätes des Hausnetzwerks integriert.

Wie bereits erwähnt wurde, kann die Schlüsseleinheit einen Speicher zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes enthalten. Bei einem Einsatz des Sicherheitssystems für den Schutz von Eigentumsrechten an digitalen Daten ist es bevorzugt, wenn die Schlüsseleinheit eine Leseeinrichtung zum Lesen eines mobilen Datenspeichers enthält. Bei dem mobilen Datenspeicher kann es sich insbesondere um eine Chipkarte handeln, auf welcher ein Dekodier-Schlüsseldatensatz gespeichert ist und welche vom Anbieter der zu schützenden digitalen Informationen regelmäßig den autorisierten Nutzern zur Verfügung gestellt wird (z. B. per gewöhnlicher Post). Durch die Ausstattung der tragbaren Einheit mit einem Kartenleser ist es möglich, unterschiedlichen Geräten eines (drahtlosen) Netzwerkes den Dekodier-Schlüsseldatensatz zur Verfügung zu stellen, ohne dass diese Geräte dazu selbst einen integrierten Kartenleser enthalten müssten.

Gemäß einer Weiterbildung der vorstehend beschriebenen Ausgestaltung kann die Schlüsseleinheit neben der Leseeinrichtung auch eine Schreibeinrichtung enthalten, mit welcher Daten auf den mobilen Datenspeicher geschrieben werden können. Dies ermöglicht es insbesondere, auf dem mobilen Datenspeicher Informationen über das Ausmaß der Nutzung der zu schützenden digitalen Informationen zu hinterlegen.

Dabei können weiterhin die tragbare Einheit und das Gerät des Netzwerkes dazu eingerichtet sein, eine Ausführungs-Bestätigung vom Gerät an die Einheit zu übertragen, wobei die Ausführungs-Bestätigung den (positiven oder negativen) Erfolg der Ausführung einer von der Einheit zuvor an das Gerät übermittelten Anweisung anzeigt. Beispielsweise kann die Ausführungs-Bestätigung anzeigen, ob ein von der Einheit an das Gerät übermittelter Schlüsseldatensatz vom Gerät erfolgreich empfangen und installiert wurde oder nicht. Ebenso kann die Ausführungs-Bestätigung anzeigen, ob die Anweisung, einen im Gerät installierten Schlüsseldatensatz zu löschen, erfolgreich ausgeführt wurde

oder nicht. Die Ausführungs-Bestätigungen erlauben somit der tragbaren Einheit, über die Installation und Aktivität von übertragenen Schlüsseldatensätzen auf dem Gerät Buch zu führen.

Vorzugsweise enthält eine Ausführungs-Bestätigung einen Identifikationscode, welcher das die Bestätigung sendende Gerät eindeutig identifiziert und hierdurch die Buchführungsfunktion der tragbaren Einheit unterstützt.

Gemäß einer anderen Weiterbildung des Sicherheitssystems mit einem mobilen Datenspeicher kann die Schlüsseleinheit der tragbaren Einheit dazu eingerichtet sein,

- Verwaltungsdaten auf dem mobilen Datenspeicher abzuspeichern, welche die Verwaltung der aus dem Datenspeicher gelesenen und auf Geräten installierten Schlüsseldatensätze erlauben, und
- die Übertragung eines Schlüsseldatensatzes vom mobilen Datenspeicher zu einem Gerät dann zu sperren, wenn die genannten Verwaltungsdaten ein vorgegebenes Kriterium erfüllen.

Die vorstehend beschriebene Ausgestaltung des Sicherheitssystems ermöglicht einen besonders umfassenden Schutz von Eigentumsrechten an digitalen Daten. Dies geschieht zum einen dadurch, dass alle die Nutzung eines Dekodier-Schlüsseldatensatzes, der auf dem mobilen Datenspeicher gespeichert ist, betreffenden Nutzungsdaten wiederum auf dem mobilen Datenspeicher hinterlegt werden. Zusammen mit dem mobilen Datenspeicher ist somit jederzeit die Information verfügbar, wie oft der Dekodier-Schlüsseldatensatz schon auf irgendwelchen Geräten oder auf unterschiedlichen Geräten installiert wurde bzw. dort aktiv ist. Wenn diese Nutzungsdaten dabei ein vorgegebenes Kriterium erfüllen, kann die weitere Übertragung von Schlüsseldatensätzen aus dem mobilen Datenspeicher an ein Gerät gesperrt werden. Beispielsweise kann das Kriterium darin bestehen, dass der Schlüsseldatensatz auf nicht mehr als N (= 1, 2, 3, ...) unterschiedlichen Geräten installiert und aktiv sein darf. Wichtig ist dabei auch, dass die erforderlichen Nutzungsdaten auf dem mobilen Datenspeicher selbst hinterlegt werden (und nicht

etwa nur in der tragbaren Einheit), sodass die Nutzungsbeschränkungen der Dekodier-Schlüsseldatensätze nicht durch den Wechsel des mobilen Datenspeichers in ein anderes Lesegerät umgangen werden können.

Des Weiteren kann die tragbare Einheit eine Auslöseeinheit enthalten, bei deren Betätigung das Gerät zum Löschen eines Schlüsseldatensatzes veranlasst wird. Auf diese Weise ist es zum Beispiel möglich, einen zuvor an das Gerät übertragenen Dekodier-Schlüsseldatensatz wieder zu deinstallieren, sodass unter Einhaltung der Nutzungsbeschränkungen der Dekodier-Schlüsseldatensatz woanders neu installiert werden kann.

Die Erfindung betrifft auch eine tragbare Einheit zur Installation eines vorzugsweise gemeinsamen Schlüssels in wenigstens einem Gerät eines (insbesondere drahtlosen) Netzwerkes, die eine Schlüsseleinheit zur Bereitstellung eines Schlüsseldatensatzes enthält und die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist.

Die Einheit kann insbesondere so weitergebildet werden, dass sie in einem Sicherheitssystem der oben erläuterten Art verwendet werden kann.

Weiterhin betrifft die Erfindung ein elektrisches Gerät mit einer Empfangseinheit, die einen Empfänger zum Empfang eines Schlüsseldatensatzes und eine Auswertekomponente des Gerätes zur Speicherung, Weiterleitung und/oder Verarbeitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.

Das elektrische Gerät kann insbesondere so weitergebildet werden, dass es in einem Sicherheitssystem der oben erläuterten Art verwendet werden kann.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Abbildungen näher erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung von drei Einheiten und eines Gerätes,

Fig. 2 Blockschaltbild einer Einheit als Sendeeinheit bei Verwendung von Hochfrequenz-Transpondertechnologie,

Fig. 3 Blockschaltbild einer Einheit als Empfangs- und Sendeeinheit bei Verwendung von Hochfrequenz-Transpondertechnologie,

Fig. 4 Blockschaltbild einer Einheit als eine Gästeeinheit bei Verwendung von Hochfrequenz-Transpondertechnologie, und

Fig. 5 den Einsatz des Sicherheitssystems für ein Digital Rights Management (DRM).

Anhand Fig. 1 wird die Installation eines elektrischen Gerätes in ein Hausnetzwerk, das aus hier nicht dargestellten, drahtlosen und drahtgebundenen Geräten besteht, beschrieben. Dargestellt sind eine erste, tragbare Einheit 1, eine Gästeeinheit 13, eine DRM-Einheit 101 und ein Personal-Computer (PC) 2 als ein im Hausnetzwerk neues Gerät. Die drahtlosen Geräte des Hausnetzwerks besitzen alle entsprechende, am Beispiel des PCs 2 beschriebene Komponenten 8 bis 12.

Die erste Einheit 1 besteht aus einer Schlüsseleinheit in Form eines Speichers 3 zur Speicherung eines Schlüsseldatensatzes 4, einer ersten Taste 5 als eine Einheit zur Auslösung einer Schlüsselübertragung und einem ersten Sender 6, der als eine drahtlose Schnittstelle zum Aussenden des Schlüsseldatensatzes 4 dient. Die Einheit 1 zeichnet sich durch ihre kurze Reichweite von maximal etwa 50 cm aus.

Die Gästeeinheit 13 beinhaltet eine Schlüsseleinheit 3 mit einer als Schlüsselgenerator 14 bezeichneten Komponente zur Erzeugung von Schlüsseldatensätzen, z.B. nach dem Zufallsprinzip, eine zweite Taste 15 und einen zweiten Sender 16. Die Gästeeinheit 13 ermöglicht Gästen mit eigenen Geräten (die nicht zum Hausnetzwerk gehören) einen ggf. nur beschränkten Zugriff auf die Geräte und Anwendungen des Hausnetzwerks. Deshalb wird ein durch den Schlüsselgenerator 14 erzeugter Schlüsseldatensatz als Gast-Schlüsseldatensatz 17 bezeichnet.

Die DRM-Einheit 101 beinhaltet eine Schlüsseleinheit 103 mit einem Speicher 103a zur Speicherung eines Schlüsseldatensatzes und mit einem Schreib-/Lesegerät 107, welches eine eingeführte Chipkarte 108 lesen und beschreiben kann. Ferner beinhaltet die DRM-Einheit 101 eine erste Taste 105a, mit welcher die Übertragung eines (Heim-)Schlüsseldatensatzes aus dem Speicher 103a ausgelöst werden kann, eine zweite Taste 105b, mit welcher die Übertragung eines Schlüsseldatensatzes von der Chipkarte 108 ausgelöst werden kann, eine dritte Taste 105c, mit welcher an ein Gerät eine Anweisung zum Löschen eines Schlüsseldatensatzes gesandt werden kann, und eine Sende-/Empfangseinheit 106 zur Übermittlung von Schlüsseldatensätzen 104 an ein Gerät und zum Empfangen von Rückmeldungssignalen 104' vom Gerät. Auf die Funktion der DRM-Einheit 101 wird unten in Zusammenhang mit Figur 5 näher eingegangen.

Der PC 2 ist ein mit einer nach dem IEEE802.11-Standard arbeitenden Funkschnittstelle 12 ausgestattetes Gerät, dessen Funkschnittstelle 12 durch eine als Treibersoftware 10 bezeichnete Komponente kontrolliert wird und zur Übertragung von Nutzdaten (Musik, Video, allgemeine Daten, aber auch Steuerdaten) dient. Die Treibersoftware 10 kann über standardisierte Softwareschnittstellen (APIs) von anderen Softwarekomponenten angesprochen werden. Zusätzlich ist der PC 2 mit einer Empfangseinheit 7 ausgestattet. Die Empfangseinheit 7 besteht aus einem Empfänger 9, der als Schnittstelle zum Empfang der von Sendern 6, 16 oder 106 gesendeten Schlüsseldatensätze 4, 17 oder 104 vorgesehen ist. In der Empfangseinheit 7 ist als Auswertekomponente eine Empfängersoftware 11 vorgesehen, die nach Erhalt eines Schlüsseldatensatzes aus diesem einen Schlüssel 18 (z. B einen in dem IEEE802.11 Standard definierten Wired Equivalent Privacy (WEP)-Schlüssel) extrahiert und diesen Schlüssel 18 über eine standardisierte Management-Schnittstelle (als MIB (Management Information Base) - Attribut beim IEEE802.11-Standard) an die Treibersoftware 10 weiterleitet. Der PC 2 weist eine zum Betrieb des PCs notwendige Anwendungssoftware 8 auf.

Ein Benutzer möchte den PC 2 ins Hausnetzwerk installieren und drahtlos mit einer HiFi-Anlage des Hausnetzwerkes verbinden, damit er mehrere im PC 2 gespeicherte Musikdateien im MP3-Format auf seiner HiFi-Anlage abspielen kann. Dazu begibt sich der Benutzer mit der Einheit 1 in die Nähe des PCs 2 und startet eine Übertragung des im Speicher 3 gespeicherten Schlüsseldatensatzes 4, indem er aus einer Entfernung von einigen Zentimetern den Sender 6 der Einheit 1 auf den Empfänger 9 richtet und die Taste 5 der Einheit 1 betätigt.

Bei der Übertragung des Schlüsseldatensatzes 4 werden Infrarotsignale verwendet. Das Format des Schlüsseldatensatzes 4 ist eine 1024 Bit-Sequenz, aus welcher die Empfängersoftware 11 die 128 low-order Bits extrahiert und als (WEP-)Schlüssel 18 an die Treibersoftware 10 weiterleitet. In der Treibersoftware 10 wird dieser Schlüssel 18 zur Verschlüsselung des Datenverkehrs zwischen dem PC 2 und der HiFi-Anlage sowie anderen Geräten, bei denen ebenfalls die Eingabe des Schlüsseldatensatzes 4 stattgefunden hat, verwendet. Dies bezieht sich auch auf die nachfolgend zur Auto-Konfiguration der Netzwerkanbindung des PCs an das Hausnetz (z.B. Konfiguration einer IP-Adresse) notwendige Kommunikation mit den schon im Netzwerk vorhandenen Geräten.

Verschiedene Umstände können die Installation eines neuen Schlüssels erfordern, z.B. wenn die Einheit dem Benutzer abhanden kommt, ein neues Gerät installiert werden soll oder wenn der Benutzer einen Verdacht hat, dass sein Hausnetzwerk nicht mehr geschützt ist. Grundsätzlich kann eine neue Einheit mit einem neuen Schlüsseldatensatz den zuletzt eingegebenen (alten) Schlüsseldatensatz überschreiben, wobei dann der neue Schlüsseldatensatz an allen Geräten des Hausnetzwerks neu eingegeben werden muss.

Ein missbräuchliches Eingeben eines neuen Schlüsseldatensatzes in das Hausnetz kann dadurch verhindert werden, dass mindestens ein Gerät des Hausnetzes für unbefugte Personen nicht frei zugänglich ist. Dieses Gerät kann nach der unbefugten Eingabe des neuen Schlüsseldatensatzes in die anderen Geräte des Hausnetzes nicht mehr mit diesen kommunizieren und z.B. einen entsprechenden Alarm auslösen.

Um die Sicherheit des Hausnetzwerks zu erhöhen, kann es aber auch Vorschrift sein, dass zur Eingabe eines neuen Schlüsseldatensatzes die zusätzliche Eingabe des alten Schlüsseldatensatzes 4 erforderlich ist. Dazu begibt sich der Benutzer mit der alten und der neuen Einheit in die direkte Nähe des PCs 2 oder eines anderen Gerätes des Hausnetzwerks. Der Benutzer betätigt die Taste 5 der alten Einheit 1 zur (nochmaligen) Übertragung des alten Schlüsseldatensatzes 4. Kurz darauf startet der Benutzer die Übertragung des neuen Schlüsseldatensatzes, indem er bei der neuen Einheit die Taste zur Auslösung der Übertragung betätigt.

Die Empfängersoftware 11 des PCs 2 registriert den Empfang des alten Schlüsseldatensatzes 4 und empfängt danach den neuen Schlüsseldatensatz. Nur unter der Bedingung, dass die Empfängersoftware 11 zuvor den Empfang des alten Schlüsseldatensatzes 4 registriert hat, leitet sie den neuen Schlüsseldatensatz bzw. den enthaltenen Schlüssel über die Management-Schnittstelle an die Treibersoftware 10 der Funkschnittstelle 12 weiter. Damit eine Verschlüsselung des Datenverkehrs auf Basis des neuen Schlüssels stattfinden kann, muss die oben beschriebene Eingabe des neuen Schlüsseldatensatzes an allen Geräten des Hausnetzwerks vorgenommen werden.

Ein erhöhtes Maß an Sicherheit bei der Eingabe eines neuen Schlüsseldatensatzes kann erzielt werden, wenn die Empfängersoftware 11 die Eingabe eines neuen Schlüsseldatensatzes nur akzeptiert, d.h. den enthaltenen Schlüssel weiterleitet, wenn der neue Schlüsseldatensatz mehrfach und in gewissen zeitlichen Abständen in das Gerät eingeben wird, wobei Anzahl und zeitlicher Abstand der geforderten Eingaben nur dem Benutzer bekannt sind.

Ein erhöhtes Maß an Sicherheit des Hausnetzes kann auch dadurch erzielt werden, dass ein Schlüsseldatensatz regelmäßig nach Ablauf einer gewissen Zeitspanne (mehrere Tage/Wochen/Monate) erneut an mindestens ein Gerät des Hausnetzes übertragen werden muss.

Mit Hilfe der Gästeeinheit 13 kann der Benutzer einem Gast Zugriff auf den PC 2 gewähren. Dazu begibt sich der Gast oder der Benutzer in die Nähe des PCs 2 und löst durch das Betätigen der Taste 15 eine Übertragung des durch den Schlüsselgenerator 14 erzeugten Gast-Schlüsseldatensatzes 17 aus.

Der Gast-Schlüsseldatensatz 17 besteht aus einer Bitfolge mit zusätzlichen Bits zur Übertragung weiterer Informationen. Die zusätzlichen Bits kennzeichnen den Schlüsseldatensatz als Gast-Schlüsseldatensatz und dienen zur Unterscheidung der Schlüsseldatensätze von anderen Informationen, falls die Empfangseinheit als Schnittstelle für weitere Anwendungen genutzt wird.

Die Empfangseinheit 7 empfängt den Gast-Schlüsseldatensatz 17. Die Empfängersoftware 11 identifiziert den Schlüsseldatensatz anhand der zusätzlichen Bits als Gast-Schlüsseldatensatz 17 und leitet den extrahierten Schlüssel als zusätzlichen (WEP-) Schlüssel über die Management-Schnittstelle an die Treibersoftware 10 der Funkschnittstelle 12 weiter. Die Treibersoftware 10 verwendet den Schlüssel als zusätzlichen Schlüssel zur Verschlüsselung des Datenverkehrs.

In der im IEEE802.11 Standard definierten Wired Equivalent Privacy (WEP)-Verschlüsselung ist eine parallele Verwendung von bis zu vier WEP-Schlüsseln vorgesehen. Die Geräte des Netzwerks sind in der Lage zu erkennen, welcher der WEP-Schlüssel aktuell zur Verschlüsselung verwendet wird.

Die Eingabe des Gast-Schlüsseldatensatzes 17 wird an allen Geräten des Hausnetzwerks wiederholt, die der Gast nutzen möchte, sowie an den Geräten des Gastes (z.B. Laptop), mit denen dieser Zugriff auf das Hausnetzwerk, z.B. auf die MP3-Dateien auf PC 2, erhalten möchte.

Um dem Benutzer die Kontrolle über die Dauer des gewährten Gast-Zugangs zum Hausnetz zu ermöglichen, wird automatisch nach einer festgelegten Zeitspanne (z.B. 10h) oder durch Benutzer-Interaktion (z.B. Eingabe des Heim-Schlüsseldatensatzes 4 an den Hausnetz-Geräten) der Gast-Schlüsseldatensatz 17 in den Geräten des Hausnetzwerks gelöscht.

Um eine unbefugte Benutzung eines Gast-Schlüsseldatensatzes durch einen früheren Gast zu verhindern, erzeugt der Schlüsselgenerator nach einer festgelegten Zeitspanne automatisch einen neuen Gast-Schlüsseldatensatz nach dem Zufallsprinzip.

Fig. 2 zeigt ein Blockschaltbild einer tragbaren Einheit 19 bei Verwendung einer Hochfrequenz-Transpondertechnologie zur Übertragung des Schlüsseldatensatzes 4. Die tragbare Einheit 19 besteht aus einem digitalen Teil 26, das einen Speicher 20 (wie z. B ROM) zur Speicherung des Schlüsseldatensatzes, eine Ablaufsteuerung 21 und einen Modulator 22 zur Umsetzung eines aus der Ablaufsteuerung 21 kommenden Bitstroms in zu übertragende Hochfrequenzsignale enthält. Weiterhin besteht die Einheit 19 aus einer Weiche 23 zur Trennung der durch ein als Antenne 25 bezeichnetes passives Bauelement empfangenen elektromagnetischen Energie von dem zu übertragenden Hochfrequenzsignal, einer Spannungsversorgungseinheit 24 mit Spannungsdetektor zur Versorgung des digitalen Teils 26 mit einer Betriebsspannung und der Antenne 25 zur Übertragung des aus der Weiche 23 kommenden Bitstroms als auch zum Empfang der für den Betrieb notwendigen Energie.

Zur Übertragung des Schlüsseldatensatzes 4 begibt sich der Benutzer mit der tragbaren Einheit 19 in unmittelbare Nähe der Empfangseinheit 7. Die Antenne 25 leitet die einströmende Energie von der Empfangseinheit 7 über die Weiche 23 an die Spannungsversorgungseinheit 24 mit Spannungsdetektor weiter. Falls ein Schwellenwert der Spannung in dem Spannungsdetektor überschritten wird, sorgt die Spannungsversorgungseinheit 24 für eine Betriebsspannung in der Einheit 19. Durch die Betriebsspannung angeregt wird die Ablaufsteuerung 21 initialisiert und liest den in dem Speicher 20 gespeicherten

Schlüsseldatensatz aus. Der Schlüsseldatensatz wird durch die Ablaufsteuerung 21 in ein geeignetes Nachrichtenformat eingebettet und an den Modulator 21 zur Umwandlung in analoge Hochfrequenzsignale weitergeleitet. Die Hochfrequenzsignale werden über die Weiche 23 durch die Antenne 25 ausgesendet.

In Fig. 3 ist die Einheit 19 als Empfangs- und Sendeeinheit bei Verwendung der gleichen Technologie wie in Fig. 2 dargestellt. In dieser Darstellung sind gleiche oder entsprechende Elemente und Komponenten wie in Fig. 2 jeweils mit gleichen Bezugsziffern bezeichnet. Insoweit wird auf die Beschreibung im Zusammenhang mit Fig. 2 Bezug genommen, und nachfolgend werden nur die Unterschiede erläutert.

In dieser Ausführungsform weist die Einheit 19 neben dem Modulator 21 einen Demodulator 27 auf. Der Speicher 20 wird durch einen löschbaren Speicher wie z.B. einen elektrisch löschbaren Speicher eines EEPROM realisiert.

Durch den Demodulator 27 ist die Einheit 19 in der Lage, ein durch die Antenne 25 (zusätzlich zur einströmenden Energie) empfangenes und über die Weiche 23 weitergeleitetes Hochfrequenzsignal in eine Bitfolge umzusetzen. Die vom Demodulator 27 kommende Bitfolge wird durch die Ablaufsteuerung 21 verarbeitet. Die Verarbeitung der Bitfolge kann in einem Zugriff der Ablaufsteuerung 21 auf den Speicher 20 resultieren, falls die Ablaufsteuerung 21 feststellt, dass die Bitfolge Informationen enthält, die die Empfangseinheit zum Empfang des Schlüsseldatensatzes berechtigen. Falls die Empfangseinheit berechtigt ist, den Schlüsseldatensatz zu empfangen, liest die Ablaufsteuerung 21 den Schlüsseldatensatz aus und leitet ihn wie in Fig. 2 beschrieben zur Aussendung an die Antenne 25 weiter.

Durch den Demodulator 27 ist es des weiteren möglich, einen neuen Schlüsseldatensatz in die Einheit 19 einzubringen. Wird der Speicher 20 als beschreibbarer Speicher (z.B. EEPROM) realisiert, lässt sich auf diese Weise der in der Einheit 19 enthaltene Schlüsseldatensatz durch einen neuen Schlüsseldatensatz ersetzen.

In Fig. 4 ist die Einheit 19 als eine Gästeeinheit 28 bei Verwendung der gleichen Technologie wie in Fig. 2 dargestellt. In dieser Darstellung sind ebenfalls gleiche oder entsprechende Elemente und Komponenten wie in Fig. 3 jeweils mit gleichen Bezugsziffern bezeichnet. Insoweit wird auf die Beschreibung im Zusammenhang mit Fig. 3 Bezug genommen, und nachfolgend werden nur die Unterschiede erläutert. Die Gästeeinheit 28 weist zusätzlich einen Schlüsselgenerator 29 auf, der mit der Ablaufsteuerung 21 verbunden ist und zur Erzeugung einer Folge von Gastschlüsseldatensätzen dient.

Nachdem die durch die Antenne 25 in unmittelbarer Nähe der Empfangseinheit 7 einströmende Energie in der Spannungsversorgungseinheit 24 mit Spannungsdetektor detektiert wurde, wird die digitale Einheit 26 durch die Spannungsversorgungseinheit 24 mit einer Betriebsspannung versorgt. Die Ablaufsteuerung 21 liest einen durch den Schlüsselgenerator 29 erzeugten Schlüsseldatensatz ein. Nachdem die Ablaufsteuerung 21 den Schlüsseldatensatz erhalten hat und in ein geeignetes Nachrichtenformat eingebettet hat, leitet sie ihn weiter zur Versendung an den Modulator 22 und schreibt gleichzeitig den Schlüsselsatz in den Speicher 20 ein, der für diesen Zweck als beschreibbarer Speicher ausgeführt sein muss (z.B. EEPROM).

In einer zweiten Betriebsart wird vom Schlüsselgenerator in regelmäßigen Abständen (zum Beispiel einige Minuten oder Stunden) ein neuer Schlüsseldatensatz erzeugt und im wiederbeschreibbaren Speicher 20 abgelegt. Der weitere Ablauf entspricht dann den Erläuterungen wie zu Fig. 2 und Fig. 3 angegeben.

Die Ausführungsform der Einheit 19 mit Schlüsselgenerator wie in Fig. 4 gezeigt ist auch mit der in Fig. 2 gezeigten Ausführungsform (ohne Demodulator 27) kombinierbar.

Figur 5 zeigt schematisch die Komponenten, die beim Einsatz des Sicherheitssystems zum Schutz von Eigentumsrechten an digitalen Daten beteiligt sind. Derzeit erfolgt der Schutz von Eigentumsrechten bzw. das Digital Rights Management (DRM) wie folgt: Der Anbieter der digitalen Daten 111 (z. B. Pay TV) sendet diese - zum Beispiel über

einen Satelliten 110 - mit einem nur ihm bekannten Schlüssel verschlüsselt aus. Die verschlüsselten Daten 111 können von einem geeigneten Empfänger 112 empfangen und an ein Gerät 113 wie etwa eine Settop-Box weitergeleitet werden. Um den Inhalt der verschlüsselten Daten nutzen zu können, muss das Gerät 113 den geheimen Schlüssel des Datenanbieters kennen. Die Bereitstellung dieses Schlüssels erfolgt über eine Chipkarte 108, welche vom Datenanbieter den berechtigten und bezahlenden Nutzern zum Beispiel monatlich per Post übersandt wird. Die Chipkarte 108 kann dann in einen mit dem Gerät 113 verbundenen Kartenleser eingeführt werden, woraufhin das Gerät 113 den auf der Karte abgelegten Dekodier-Schlüsseldatensatz lesen und verwenden kann. Charakteristisch für dieses System ist, dass die zu schützenden Daten das Gerät 113 nicht in digitaler, unverschlüsselter Form verlassen dürfen, damit ihre Nutzung mit dem Besitz der Chipkarte 108 gekoppelt und somit kontrollierbar ist.

Andererseits besteht jedoch bei modernen digitalen Netzwerken zunehmend der Wunsch, Daten auf verschiedenen Geräten nutzen zu können, insbesondere auf drahtlos ans Netzwerk gekoppelten Geräten. Damit hierfür nicht auf jedem derartigen Gerät ein Kartenleser eingerichtet werden muss, wird die DRM-Einheit 101 (Figur 1, Figur 5) eingesetzt. Diese enthält, wie in Zusammenhang mit Figur 1 bereits erläutert wurde, einen Kartenleser 107 (ähnlich den SIM Kartenlesern in Mobiltelefonen), welcher die Chipkarte 108 lesen und vorzugsweise auch beschreiben kann. Die DRM-Einheit 101 kann daher insbesondere den auf der Chipkarte 108 hinterlegten Dekodier-Schlüsseldatensatz auslesen und mittels einer Kurzstreckenübertragung an den entsprechend eingerichteten Empfänger 107 eines Gerätes 102 übertragen. Das Gerät 102 kann dann (wenn es die entsprechend Software enthält) mit Hilfe des Dekodier-Schlüsseldatensatzes 104 die verschlüsselten Daten 109 entschlüsseln, welche der oben erwähnte Satellitenempfänger 112 (drahtlos) sendet. Die Nutzung dieser Daten 109 ist daher auch auf dem Gerät 102 möglich, ohne dass dieses hierzu ein eigenes Kartenlesegerät enthalten müsste.

Das beschriebene System kann ferner dahingehend weitergebildet werden, dass es eine nicht autorisierte mehrfache Übertragung eines Dekodier-Schlüsseldatensatzes 104 an verschiedene Geräte verhindert. Dies kann gemäß einer ersten Ausführungsform so

geschehen, dass der Dekodier-Schlüsseldatensatz 104 auf dem Gerät 102 in regelmäßigen, verhältnismäßig kurzen Zeitabständen verfällt bzw. automatisch gelöscht wird, sodass er quasi ständig neu von der DRM-Einheit 101 übertragen werden muss. Eine gleichzeitige Nutzung mehrerer Geräte wäre damit praktisch ausgeschlossen.

Bei einer fortgeschritteneren Nutzungskontrolle erfolgt eine bidirektionale Kommunikation zwischen der DRM-Einheit 101 und dem Gerät 102. Dabei antwortet das Gerät 102 jedes Mal, wenn es von der DRM-Einheit 101 einen Schlüsseldatensatz 104 empfangen und erfolgreich installiert hat, mit einer Ausführungsbestätigung 104', welche die erfolgreiche Übernahme des Schlüsseldatensatzes anzeigt sowie einen Identifikationscode ID für das Gerät 102 enthält. Dieser ID wird dann von der DRM-Einheit 101 auf der Chipkarte 108 abgespeichert. Wenn eine vorgegebene erlaubte Anzahl an aktivierbaren Geräten erreicht ist (diese Anzahl kann z.B. auf der Chipkarte hinterlegt sein), kann dies die DRM-Einheit 101 erkennen und als Reaktion hierauf keinen weiteren Dekodier-Schlüsseldatensatz 104 an irgendein Gerät mehr senden.

Ein erneutes Senden von Dekodier-Schlüsseldatensätzen durch die DRM-Einheit 101 wird erst dann wieder möglich, wenn die Anzahl an Geräten mit aktivierten Schlüsseldatensätzen abnimmt. Dies kann zum Beispiel automatisch nach Ablauf vorgegebener Zeitspannen der Fall sein. Vorzugsweise enthält die DRM-Einheit 101 jedoch eine "Löschtaste" 105c (Figur 1), nach deren Betätigung eine Interaktion mit einem Zielgerät 102 stattfindet. Dabei wird zunächst von der DRM-Einheit 101 die ID des Gerätes 102 angefordert. Das Gerät 102 sendet daraufhin seine ID, welche von der DRM-Einheit 101 empfangen und mit den auf der Chipkarte 108 gespeicherten IDs von Geräten mit aktiviertem Schlüsseldatensatz verglichen wird. Falls die ID auf der Karte vorhanden ist, sendet die DRM-Einheit eine Anweisung an das Gerät 102, den Dekodier-Schlüsseldatensatz im Gerät zu löschen. Eine vom Gerät 102 daraufhin ausgesandte Ausführungs-Bestätigung teilt der DRM-Einheit 101 mit, ob das Löschen wie gewünscht ausgeführt wurde oder nicht. Falls erfolgreich gelöscht wurde, kann die ID des Gerätes 102 von der Chipkarte 108 gelöscht werden, sodass anschließend die Nutzung des Dekodier-Schlüsseldatensatzes auf einem anderen Gerät möglich ist.

PATENTANSPRÜCHE

1. Sicherheitssystem für Netzwerke, insbesondere drahtlose Netzwerke, mit

- einer tragbaren Einheit (1, 13, 101), die eine Schlüsseleinheit (3, 103) zur Bereitstellung eines Schlüsseldatensatzes (4, 17, 104) enthält und die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4, 17, 104) vorgesehen ist, und
- mindestens einer Empfangseinheit (7, 107) in wenigstens einem Gerät (2, 102) des Netzwerks, die einen Empfänger (9) zum Empfang des Schlüsseldatensatzes (4, 17, 104) und eine Auswertekomponente (11) des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes (4, 17, 104) oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.

2. Sicherheitssystem nach Anspruch 1,
dadurch gekennzeichnet,
dass die Einheit (1, 13, 101) mindestens eine Auslöseeinheit (5, 15, 105a, 105b, 105c) zur Auslösung einer Kurzstreckeninformationsübertragung, insbesondere einer Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4, 17, 104), aufweist.

3. Sicherheitssystem nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass bei Annäherung an die Empfangseinheit (7, 107) eine in der Einheit (1, 13, 101) enthaltene Detektoreinheit zur Auslösung der Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4, 17, 104) vorgesehen ist.

4. Sicherheitssystem nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass die Schlüsseleinheit (3) einen Schlüsselgenerator (14) enthält, welcher zur Erzeugung einer Folge von Gast-Schlüsseldatensätzen (17) vorgesehen ist.

5. Sicherheitssystem nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass das Gerät (2, 102) zur Löschung des Schlüsseldatensatzes (17, 104) vorgesehen ist.

6. Sicherheitssystem nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass der Schlüsseldatensatz (4, 17, 104) aus einer Bitfolge besteht.

7. Sicherheitssystem nach Anspruch 6,
dadurch gekennzeichnet,
dass die Bitfolge Kennzeichnungsbits enthält, die zur Unterscheidung und Kennzeichnung von Schlüsseldatensätzen (4, 17, 104) dienen.

8. Sicherheitssystem nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass die Einheit (1, 13, 101) ein Teil eines Gerätes, insbesondere einer Fernbedienung, ist.

9. Sicherheitssystem nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
dass eine Eingabe des Schlüsseldatensatzes (4, 17, 104) während oder vor einer Netzwerkkonfiguration, insbesondere einer automatischen Netzwerkkonfiguration, eines Gerätes (2, 102) vorgesehen ist.

10. Sicherheitssystem nach mindestens einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass das Gerät (2, 102) mittels eines im Schlüsseldatensatz (4, 17, 104) enthaltenen Schlüssels zur Authentifizierung, Verschlüsselung und/oder Entschlüsselung von zwischen den Geräten des Netzwerks übertragenen Nutzdaten (109) vorgesehen ist.

11. Sicherheitssystem nach mindestens einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass die Schlüsseleinheit einen Speicher (3, 103a) zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes (4, 104) enthält.

12. Sicherheitssystem nach mindestens einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Schlüsseleinheit (103) eine Leseeinrichtung (107) zum Lesen eines mobilen Datenspeichers, insbesondere einer Chipkarte (108) mit einem darauf gespeicherten Dekodier-Schlüsseldatensatz (104), enthält.

13. Sicherheitssystem nach Anspruch 12, dadurch gekennzeichnet, dass die Schlüsseleinheit (3) eine Schreibeinrichtung (107) zum Schreiben von Daten auf den mobilen Datenspeicher (108) enthält.

14. Sicherheitssystem nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass die Einheit (101) und das Gerät (2, 102) zur Übertragung einer Ausführungs-Bestätigung (104') vom Gerät (2, 102) an die Einheit (101) eingerichtet sind, welche den Erfolg der Ausführung einer von der Einheit (101) an das Gerät (2, 102) übermittelten Anweisung anzeigt.

15. Sicherheitssystem nach Anspruch 14,
dadurch gekennzeichnet,
dass die Ausführungs-Bestätigung (104') einen Identifikationscode für das Gerät (2, 102) enthält.

16. Sicherheitssystem nach Anspruch 13,
dadurch gekennzeichnet,
dass die Schlüsseleinheit (3) dazu eingerichtet ist,

- Nutzungsdaten auf dem mobilen Datenspeicher (108) abzuspeichern, welche die Verwaltung der vom Datenspeicher (108) gelesenen und auf Geräten (2, 102) installierten Schlüsseldatensätze (104) erlauben, und
- die Übertragung eines Schlüsseldatensatzes (104) vom mobilen Datenspeicher (108) zu einem Gerät (2, 102) zu sperren, falls die genannten Nutzungsdaten ein vorgegebenes Kriterium erfüllen.

17. Sicherheitssystem nach Anspruch 5,
dadurch gekennzeichnet,
dass die Einheit (101) eine Auslöseeinheit (105c) enthält, bei deren Betätigung sie das Gerät (2, 102) zum Löschen eines Schlüsseldatensatzes (104) veranlasst.

18. Tragbare Einheit (1, 13, 101) zur Installation eines Schlüssels in wenigstens einem Gerät (2, 102) eines vorzugsweise drahtlosen Netzwerkes, die eine Schlüsseleinheit (3, 103) zur Bereitstellung eines Schlüsseldatensatzes (4, 17, 104) enthält und die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist.

19. Elektrisches Gerät (2, 102) mit einer Empfangseinheit (7, 107), die einen Empfänger (9) zum Empfang eines Schlüsseldatensatzes (4, 17, 104) und eine Auswertekomponente (11) des Gerätes (2, 102) zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente (10) aufweist.

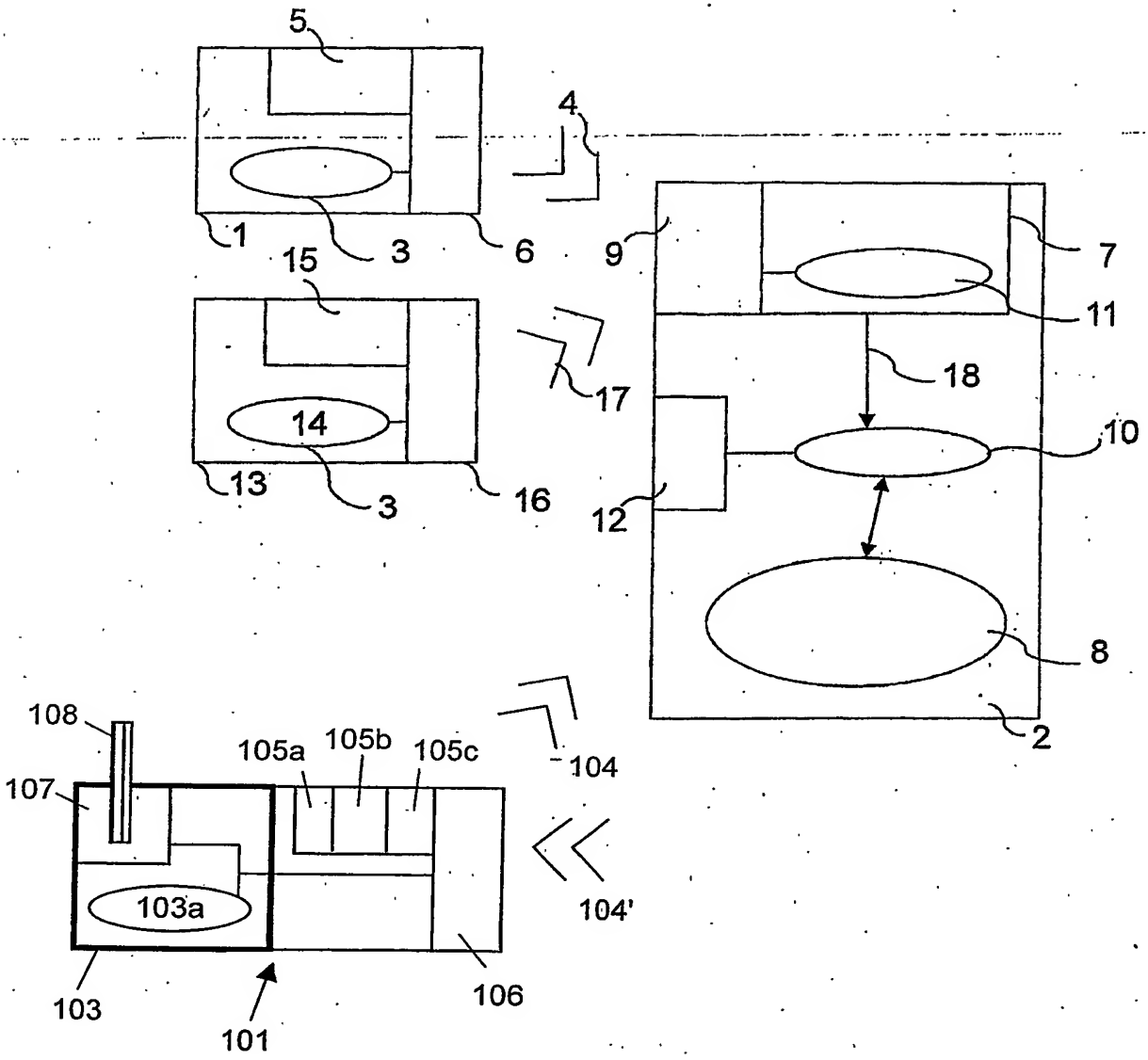

5
4
1
3
6
9
7
11
15
18
17
14
10
13
3
16
12
8
2
108
105a
105b
105c
104
107
103a
104'
103
101
106

FIG. 1

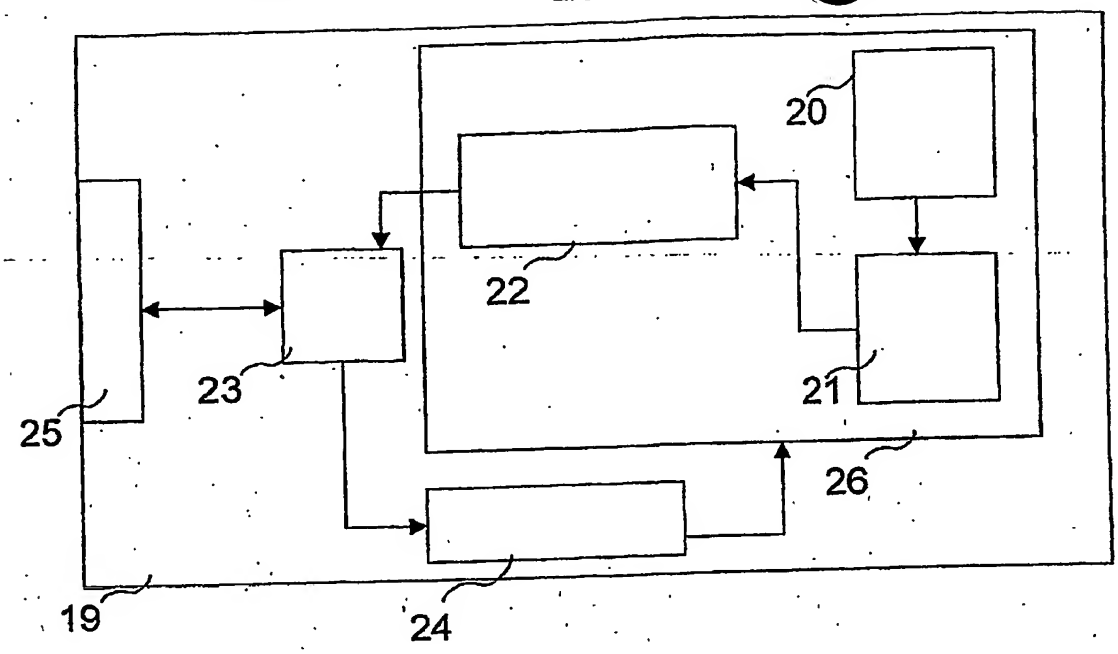

20
22
23
21
25
26
19
24

FIG. 2

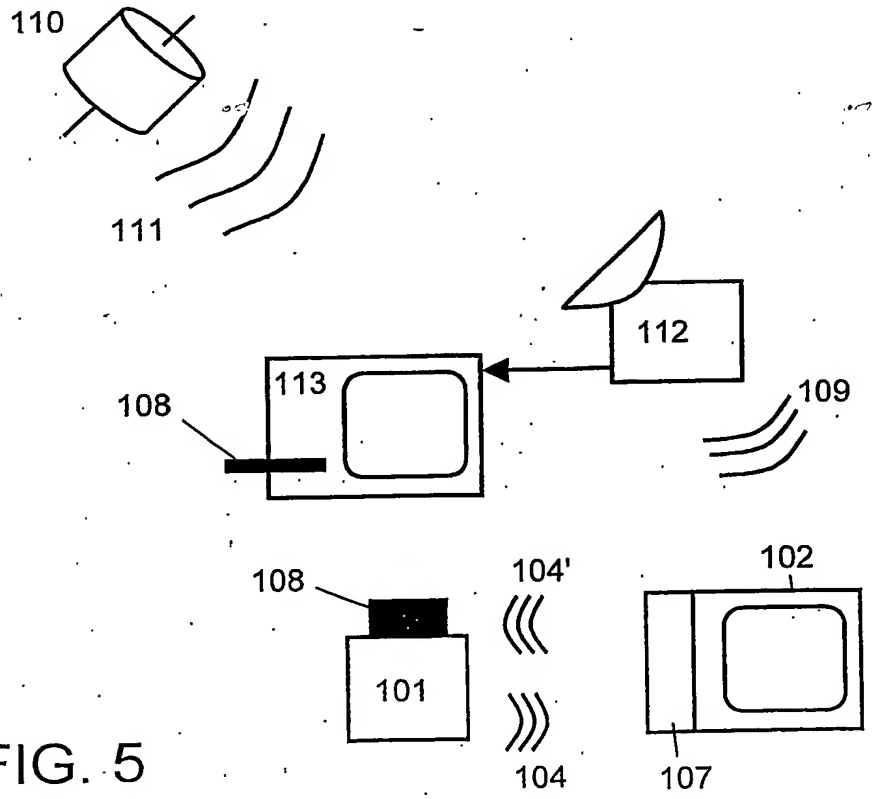

110
111
112
113
108
109
108
104'
102
101
104
107

FIG. 5

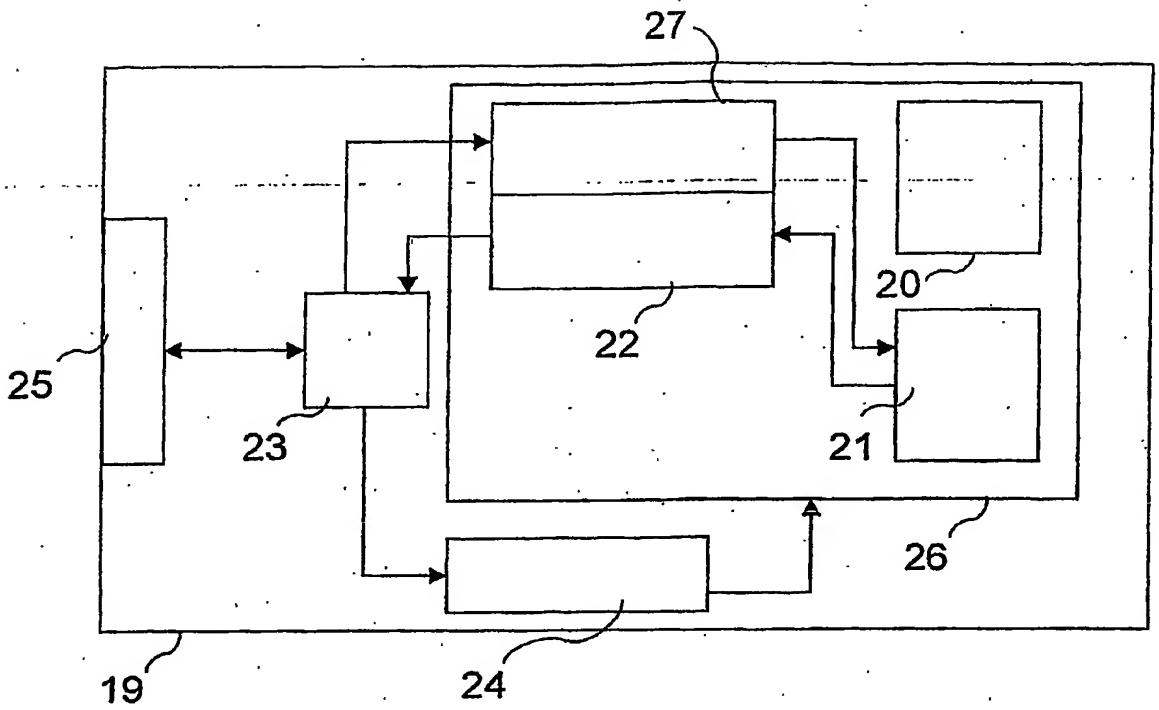


FIG. 3

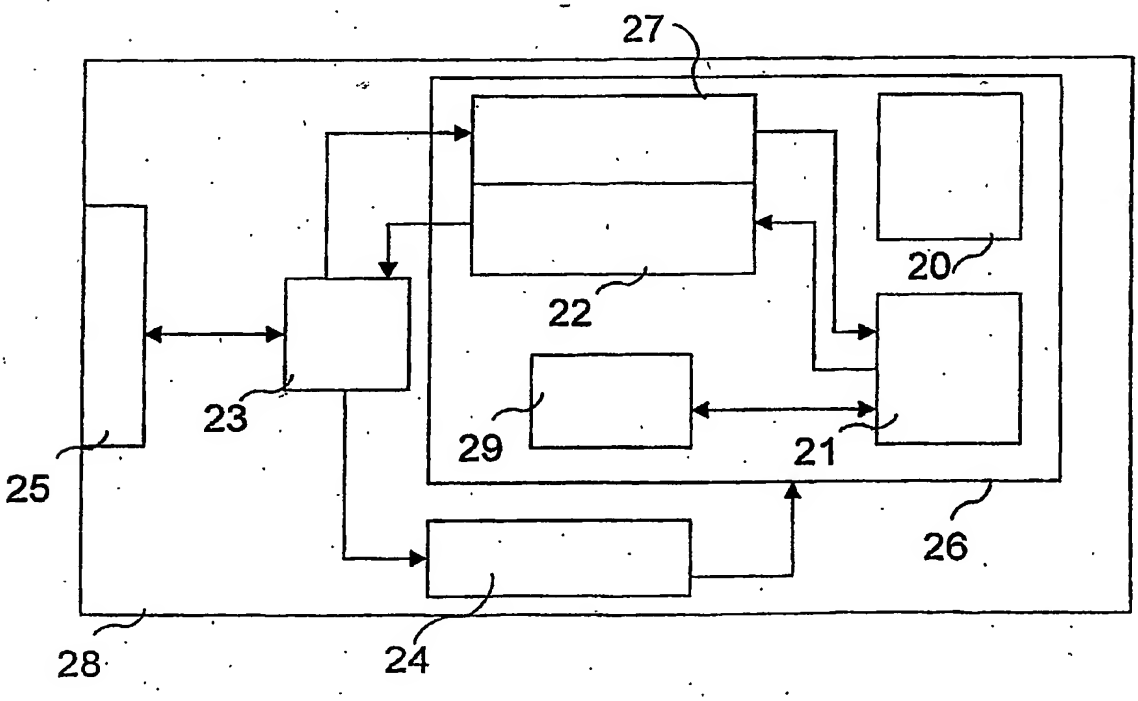


FIG. 4